UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,074	03/26/2001	W. Dale Hopkins	20206-15 (P00-3323)	9764

7590 09/09/2004

Hewlett-Packard Company
Attn. Bill Streeter
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 09/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/818,074	HOPKINS ET AL.	
	Examiner	Art Unit	
	Andrew L Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 10-15, 17-18, 20, and 38-39* is/are rejected.

7)☒ Claim(s) *2-9,16,19,21-37 and 40-43* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/26/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-43 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1 and 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Boesch US Patent No. 6,125,185. Boesch discloses a system for encryption key generation.

4. With regards to claims 1 and 20, Boesch teaches the pre-computing of one or more different types of sets of cryptographic parameters each of said type of set being adapted for use by an associated type of cryptographic application (Boesch, column 5 lines 1-5, computes DES keys for different receiving parties), securely storing said pre-computed sets of cryptographic parameters in a memory storage unit (Boesch, column 5 lines 9-12), receiving a request for a set of cryptographic parameters having specified characteristics for use in a particular cryptographic application (Boesch, column 5 lines 13-20), determining one of said sets of cryptographic parameters stored in said memory storage unit that has specified characteristics (Boesch, column 5 lines 13-20), accessing said determined set of cryptographic parameters from said memory storage

unit (Boesch, column 5 lines 14-15), and providing said determined set of cryptographic parameters with minimal latency (Boesch, column 5 lines 13-15, column 4 lines 51-67).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Boesch US Patent No. 6,125,185 in view of Collins et al US Patent No. 5,848,159.

7. With regards to claim 10, Boesch teaches the step of pre-computing (Boesch, column 5 lines 1-5), but fails to teach the generation of k prime numbers and the performing of at least one probabilistic primality test. Collins teaches the set of parameters including an associated number k or randomly generated prime numbers wherein $k \geq 1$ (Collins, column 5 lines 51-67 "p1, p2, p3"), wherein the step of computing is performed by a processing unit with a plurality of exponentiation units communicatively coupled with the processing unit (Collins, Figure 1 Items 32a, 32b, 32c), randomly generating a plurality of k random odd numbers each being a prime number candidate (Collins, column 5 lines 30-32), and performing at least one probabilistic primality test on each of the candidates, each of the primality tests including an associated exponentiation operation executed by an associated one of the exponentiation units (Collins, column 5 lines 32-33, checked to ensure each is prime),

and the exponentiation operations being performed in parallel (Collins, column 5 lines 30-33, Figure 1 Items 32a, 32b, 32c). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Collins' method of generating random prime numbers and performing probabilistic primality tests upon them with Boesch's key generation system because it offers the advantage of increasing the key generation efficiency by providing the ability to generate a large public key by using small prime number components (Collins, column 3 lines 36-55).

8. Claims 17-18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Boesch US Patent No. 6,125,185 in view of Hori et al US Patent No. 6,578,057.

9. With regards to claim 17, Boesch teaches everything that is described above, but fails to disclose the cryptographic parameters being prime number values. Hori discloses the generation of prime numbers suitable for use in a cryptographic security application (Hori, column 4 lines 46-65). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Hori's method of prime number generation with Boesch's key generation system because it offers the advantage of providing a method of generating prime numbers that are beneficial for message authentication and user validation (Hori, column 1 lines 16-23).

10. With regards to claim 18, Boesch as modified teaches the computing of random distinct prime numbers with different lengths (Hori, column 5 lines 46-56, rank), receiving a request including an associated specified length (Hori, column 5 lines 46-56, rank), and determining at least one of the securely stored prime number values that has

the associated specified length and accessing the at least one determined prime number value from the memory storage unit (Hori, column 5 line 65 – column 6 line 45).

11. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boesch US Patent No. 6,125,185 in view of Collins et al US Patent No. 5,848,159 and Hori et al US Patent No. 6,578,057.

12. With regards to claim 11, Boesch teaches the step of pre-computing (Boesch, column 5 lines 1-5), but fails to teach the generation of k prime numbers and the performing of at least one probabilistic primality test. Collins teaches the set of parameters including an associated number k or randomly generated prime numbers wherein $k \geq 1$ (Collins, column 5 lines 51-67 "p1, p2, p3"), wherein the step of computing is performed by a processing unit with a plurality of exponentiation units communicatively coupled with the processing unit (Collins, Figure 1 Items 32a, 32b, 32c), randomly generating a plurality of k random odd numbers each being a prime number candidate (Collins, column 5 lines 30-32), and performing at least one probabilistic primality test on each of the candidates, each of the primality tests including an associated exponentiation operation executed by an associated one of the exponentiation units (Collins, column 5 lines 32-33, checked to ensure each is prime), and the exponentiation operations being performed in parallel (Collins, column 5 lines 30-33, Figure 1 Items 32a, 32b, 32c). Hori discloses the determining of a plurality of y additional odd numbers based on the at least one randomly generated odd number to provide y additional prime number candidates thereby providing a number of y+1

candidates and and performing at least one probabilistic primality test on each of the candidates (Hori, column 2 lines 1-7). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Collins' method of generating random prime numbers and performing probabilistic primality tests upon them and Hori's method of producing additional prime number candidates with Boesch's key generation system because it offers the advantage of increasing the key generation efficiency by providing the ability to generate a large public key by using small prime number components (Collins, column 3 lines 36-55, Hori column 1 lines 35-39).

13. With regards to claim 12, Boesch as modified teaches the randomly generated odd number providing a random seed (Collins, column 5 lines 31-32).

14. Claims 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boesch US Patent No. 6,125,185 in view of Bergum et al US Patent No. 5,457,748.

15. With regards to claim 13, Boesch fails to teach the storing of the cryptographic parameters in a first memory unit that is protected within a logical and physical security boundary. Bergum teaches the storing of the cryptographic parameters in a first memory unit that is protected within a logical and physical security boundary (Bergum, column 3 lines 1-19 and column 3 line 63 – column 4 line 18). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Bergum's method of storing cryptographic parameters securely with Boesch's key generation system because it offers the advantage of preventing unauthorized

monitoring of communications by ensuring the security of encryption keys (Bergum, column 1 lines 37-55).

16. With regards to claim 14, Boesch as modified teaches the encrypting of at least one cryptographic parameters using a cryptographic key (Bergum, column 3 lines 4-7, master key), storing the cryptographic key in a first memory (Bergum, column 3 lines 2-4, master key stored in encryptor), and storing the cryptographic parameters in a second memory unit outside of the security boundary (Bergum, column 3 lines 4-7).

17. With regards to claim 15, Boesch as modified teaches the accessing of the encrypted cryptographic parameters from the second memory unit, accessing the cryptographic key from the first memory unit, and decrypting the accessed cryptographic parameters using the key (Bergum, column 3 lines 13-20).

18. Claims 38-39 and rejected under 35 U.S.C. 103(a) as being unpatentable over Boesch US Patent No. 6,125,185 in view of Hori et al US Patent No. 6,578,057 and Bergum et al US Patent No. 5,457,748.

19. With regards to claim 38, Boesch teaches everything that is described above and further teaches a server computing system communicatively coupled to a plurality of remote clients via a network (Boesch, column 5 lines 5-11, receiving parties), but fails to disclose the cryptographic parameters being prime number values or the secure storage of prime numbers. Hori discloses the generation of prime numbers suitable for use in a cryptographic security application (Hori, column 4 lines 46-65). Bergum teaches the storing of the cryptographic parameters in a first memory unit that is protected within a

logical and physical security boundary (Bergum, column 3 lines 1-19 and column 3 line 63 – column 4 line 18). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Hori's method of prime number generation and Bergum's method of storing cryptographic parameters securely with Boesch's key generation system because it offers the advantage of providing a method of generating prime numbers that are beneficial for message authentication and user validation (Hori, column 1 lines 16-23) and preventing unauthorized monitoring of communications by ensuring the security of encryption keys (Bergum, column 1 lines 37-55).

20. With regards to claim 39, Boesch as modified teaches the encrypting of at least one cryptographic parameters using a cryptographic key (Bergum, column 3 lines 4-7, master key), storing the cryptographic key in a first memory (Bergum, column 3 lines 2-4, master key stored in encryptor), and storing the cryptographic parameters in a second memory unit outside of the security boundary (Bergum, column 3 lines 4-7), the accessing of the encrypted cryptographic parameters from the second memory unit, accessing the cryptographic key from the first memory unit, and decrypting the accessed cryptographic parameters using the key (Bergum, column 3 lines 13-20).

Allowable Subject Matter

21. Claims 2-9, 16, 19, 21-37, 40-43 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

22. The following is a statement of reasons for the indication of allowable subject matter:

23. With regards to claims 2-9, 19, and 21-37, the present application teaches the pre-computing of different types of sets of cryptographic parameters where eat set of an associated type includes an associated number k of random generated distinct prime numbers. The cited prior art fails to teach or suggest the receiving step including receiving a request specifying characteristics including a specified number of prime number values constituting prime factors of the requested modulus where the requested number corresponds to the associated number k of random generated distinct prime numbers and thus fails to anticipate or render the above limitations obvious.

24. With regards to claim 16, the cited prior art fails to teach or suggest the request for a specified type of set of cryptographic parameters having specified characteristics where the characteristics include a specified type of Chinese Remainder Algorithm being used by the particular cryptographic application and thus fails to anticipate or render the above limitations obvious.

25. With regards to claims 40-43, the cited prior art fails to teach or suggest a system where based on the number of prime number requests and cryptographic transaction jobs currently stored in the queuing unit, and the number of cryptographic key values currently stored in the storage unit, dynamically allocating a first portion of the

exponentiation resources for prime number searching, and a second portion of the resources for processing cryptographic transactions.

Conclusion

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

27. Miller et al US Patent No. 4,351,982 discloses a RSA Public-Key data encryption system having a large random prime number generating microprocessor.

28. Torii et al US Patent No. 5,325,433 discloses an encryption communication system.

29. Venkatesan et al US Patent No. 6,091,819 discloses a system for accelerating public key cryptography by pre-computing randomly generated pairs.

30. Ober et al US Patent No. 6,307,936 discloses a cryptographic key management scheme.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 703 305 8407. After October 26, 2004, Examiner can be reached at 571 272 – 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

Andrew Caldwell
Andrew Caldwell